CLAIMS

What is claimed is:

1. A distributed architecture of an information handling system, comprising:

a buried nucleus inaccessible for inspection without heroic means while said buried nucleus is in operation; and

a trusted authority for generating a secure protocol, said secure protocol controlling operation of said buried nucleus.

2. The distributed architecture of claim 1, wherein said buried nucleus includes at least one LFSR (linear feedback shift register).

3. The distributed architecture of claim 1, wherein said buried nucleus includes at least one reconfigurable core.

4. The distributed architecture of claim 1, wherein said buried nucleus includes at least one programmable logic block.

5. The distributed architecture of claim 1, wherein said buried nucleus includes at least one non-volatile RAM.

6. The distributed architecture of claim 1, wherein said buried nucleus includes at least one matrix multiplier.

7. The distributed architecture of claim 1, wherein said trusted authority is a back-end secure server.

8. The distributed architecture of claim 1, wherein said trusted authority is a cell phone operator with a trusted command and control center.

9. The distributed architecture of claim 1, wherein said trusted authority is an encrypted medium.

10. A distributed architecture of an information handling system, comprising:

(a) a hardware/software system, comprising:

a microchip including an outer region having I/O pins and a buried nucleus inaccessible for inspection without heroic means when said buried nucleus is in operation; and

external software connected to said I/O pins for controlling said I/O pins; and

(b) a trusted authority for generating a secure protocol, said secure protocol controlling operation of said hardware/software system;

(c) wherein said buried nucleus is equipped to accept and decipher an encrypted key delivered through said secure protocol.

11. The distributed architecture of claim 10, wherein said buried nucleus includes at least one LFSR (linear feedback shift register).

12. The distributed architecture of claim 10, wherein said buried nucleus includes at least one reconfigurable core.

13. The distributed architecture of claim 10, wherein said buried nucleus includes at least one programmable logic block.

14. The distributed architecture of claim 10, wherein said buried nucleus includes at least one non-volatile RAM.

15. The distributed architecture of claim 10, wherein said buried nucleus includes at least one matrix multiplier.

16. The distributed architecture of claim 10, wherein said encrypted key is encrypted with digital watermarking.

17. The distributed architecture of claim 10, wherein said encrypted key is encrypted with a fast elliptical algorithm.

18. The distributed architecture of claim 10, wherein said encrypted key is encrypted with Triple DES.

19. The distributed architecture of claim 10, wherein said encrypted key is encrypted with a Rijndael algorithm.

20. The distributed architecture of claim 10, wherein said trusted authority is a back-end secure server.

21. The distributed architecture of claim 10, wherein said trusted authority is a cell phone operator with a trusted command and control center.

22. The distributed architecture of claim 10, wherein said trusted authority is an encrypted medium.

23. A method for protecting encrypted information, comprising steps of:

(a) setting a buried nucleus in a quasi-stable mode of operation; and

(b) stopping clocking when said buried nucleus deviates from said quasi-stable mode.

24. The method of claim 23, wherein said step (a) comprising:

(a1) delivering a key through a secure protocol to said buried nucleus;

(a2) setting up a bit string by said key; and

(a3) giving a set of timer banks a pseudorandom temporal variability by said bit string.

25. The method of claim 23, further comprising:

(c) rebuilding a secure environment within said buried nucleus after an intrusion is detected; and

(d) resetting to zero when replication of re-buildup by an attacker is detected.

26. An apparatus for protecting encrypted information, comprising:

(a) means for setting a buried nucleus in a quasi-stable mode of operation; and

(b) means for stopping clocking when said buried nucleus deviates from said quasi-stable mode.

27. The apparatus of claim 26, wherein said means (a) comprising:

(a1) means for delivering a key through a secure protocol to said buried nucleus;

(a2) means for setting up a bit string by said key; and

(a3) means for giving a set of timer banks a pseudorandom temporal variability by said bit string.

28. The apparatus of claim 26, further comprising:

(c) means for rebuilding a secure environment within said buried nucleus after an intrusion is detected; and

(d) means for resetting to zero when replication of re-buildup by an attacker is detected.

29. A computer-readable medium having computer-executable instructions for performing a method comprising steps of:

(a) setting a buried nucleus in a quasi-stable mode of operation; and

(b) stopping clocking when said buried nucleus deviates from said quasi-stable mode.

30. The computer-readable medium of claim 29, wherein said step (a) comprising:

(a1) delivering a key through a secure protocol to said buried nucleus;

(a2) setting up a bit string by said key; and

(a3) giving a set of timer banks a pseudorandom temporal variability by said bit string.

31. The computer-readable medium of claim 29, wherein said method further comprising:

(c) rebuilding a secure environment within said buried nucleus after an intrusion is detected; and

(d) resetting to zero when replication of re-buildup by an attacker is detected.